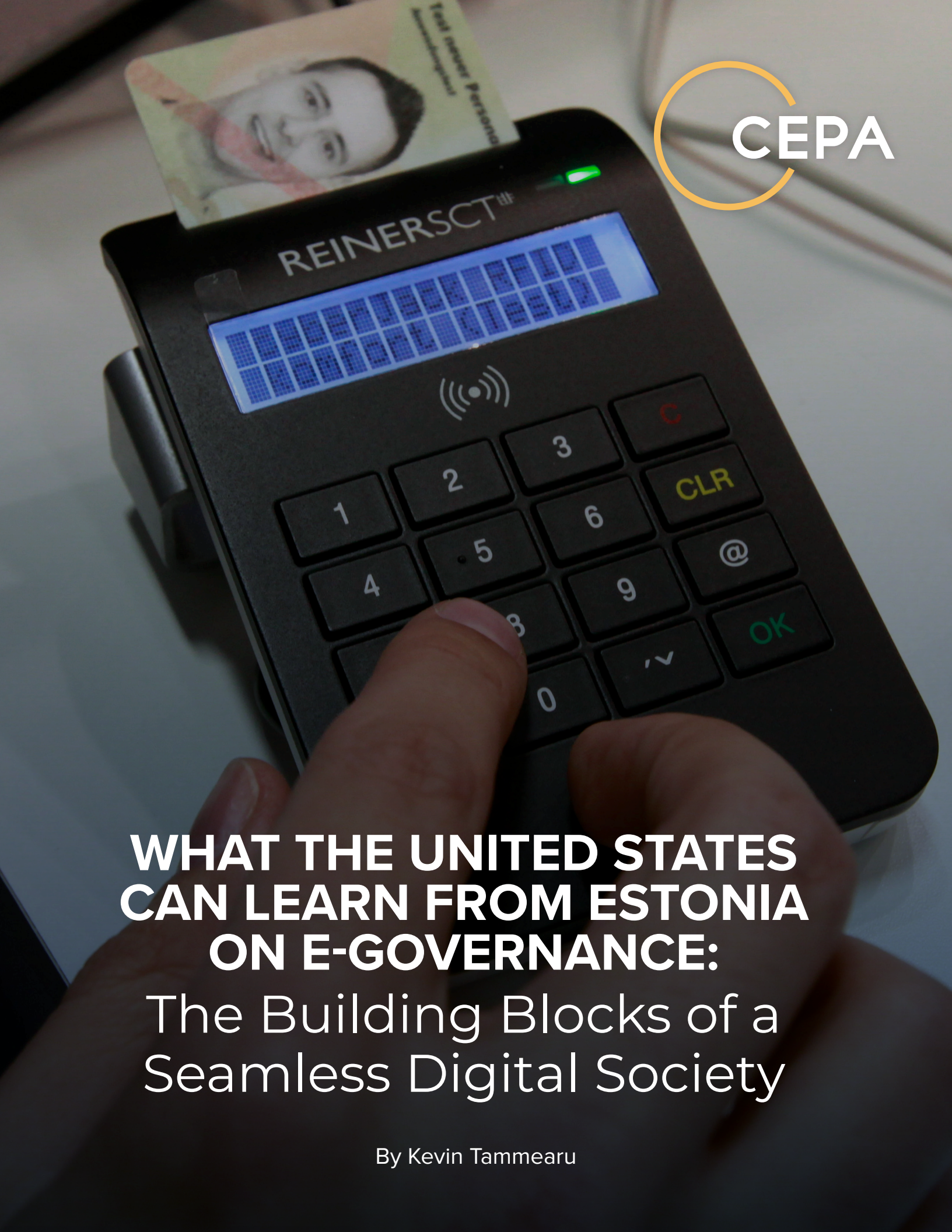

CEPA

WHAT THE UNITED STATES CAN LEARN FROM ESTONIA ON E-GOVERNANCE:

The Building Blocks of a Seamless Digital Society

By Kevin Tammearu

ABOUT CEPA

The Center for European Policy Analysis (CEPA) works to reinvent Atlanticism for a more secure future. Headquartered in Washington, D.C., and led by seasoned transatlanticists and emerging leaders from both sides of the Atlantic, CEPA brings an innovative approach to the foreign policy arena. Our cutting-edge analysis and timely debates galvanize communities of influence while investing in the next generation of leaders to understand and address present and future challenges to transatlantic values and principles. CEPA is a nonpartisan, nonprofit, public policy institution.

A man poses for photographer as he enters a PIN code for a new German ID card (Personalausweis) inserted intoa card reader, in Berlin, October 27, 2010. The card can be ordered from November 1 and offers a new so-calledeID (electronic Identity). REUTERS/Fabrizio Bensch

Contents

About the Author

Kevin Tammearu is a Digital Innovation Baltic Fellow with the Transatlantic Leadership team. Kevin is an international business professional working as Head of Business Development at Cybernetica focusing on e-governance, interoperability, and secure data exchange. Kevin works with political and business leaders across the world, assisting them in developing e-governance capabilities and strategies to address public sector challenges with digital transformation initiatives and secure technology solutions. Kevin holds a Master's in Strategic Communication from the Baltic Film, Media, Arts and Communication School of Tallinn University. Kevin's research will focus on e-governance and the instrumental building blocks for creating an environment of trust based on cohesive transatlantic policy and innovative technology measures.

Acknowledgments

This program is made possible by funding from the Baltic-American Freedom Foundation (BAFF). For more information about BAFF scholarships and programs, visit www.balticamericanfreedomfoundation.org.

The views expressed by the author are their own and do not represent the views of BAFF.

Executive Summary

- A whole-of-government approach is needed to successfully implement e-governance. The Estonian experience also shows the importance of building a strong foundation of interoperability and digital identity.
- E-government policy coordination in the United States is well developed at the federal level through the Office of Management and Budget (OMB) and the CIO Council, a forum of federal chief information officers (CIOs). Significant policy work related to federal data management, digital services, and websites has been done by OMB and GSA.
- It is not clear whether these accomplishments are enough to bring along U.S. states that have a large mandate to provide services to citizens.
- U.S. citizens are concerned about their privacy. They sense a decrease in their control of and the transparency around the use of their data.
- While there are significant differences in political and historical contexts, democratic countries share largely universal principles regarding public administration and information security. Approaches that are designed with these principles in mind can be learned from, replicated, and adapted to local contexts.

Introduction

Most sectors in the transatlantic alliance are quickly becoming digital, growing Building a 21st-century government is on U.S. policymakers' agenda — at least on paper. The last Digital Government Strategy was launched in 2012. [1] Policy goals tend to be unfulfilled as a result of a lack of funding, as is the case with the 21st Century Integrated Digital Experience (IDEA) Act.[2]

> The IDEA Act seeks to digitize services, accelerate the use of e-signatures, and improve the overall online experience of the user.[3]

Estonia has a lot of experience building a 21st-century government and a digital society.[4] It has an exceptionally well-built foundation that enables digital services. This foundation is based on government interoperability, secure data exchange, and digital identity or secure authentication and digital signatures.

This paper looks at what the United States can learn from Estonia's experience with implementing interoperability, secure data exchange, and digital identity with the goal of achieving greater trust in government, reducing the time people spend navigating bureaucracy, and protecting privacy in a way that the private sector develops further.

> E-governance refers to using technology for governance while appreciating the need to govern those technologies. E-government refers to a more narrow use of technology within government/public sector.

The United States supported Estonia's restoration of independence through the Welles Declaration and its entrance into Euro-Atlantic institutions.[5] Today, Estonia is in a position to inspire and guide the United States on how to build a more effective digital society.

e-Estonia

The term e-Estonia captures the activities and aspirations of Estonia being a cutting-edge digital society. Initially, it referred to government digital services. It later expanded to include the start-up and tech culture that emerged within the private sector.

E-Estonia has been praised as one of the most successful policy ideas in modern statecraft.[6] This whole-of-government rethinking of public services and the relationship between citizen and state has largely depended on strong political drive and the making of critical decisions when it comes to building the foundations of e-governance.

Some of the first steps toward achieving the current level of digitalization were taken in the early ’90s with the Parliament setting out a strategic outline for information technology (IT) development, including several nation-wide initiatives with the private sector. These initiatives included Tiger Leap, which sought to establish computer skills in schools, and the Look@World initiative, which targeted the wider population and their information and communications technology (ICT) skills. These initiatives and policy decisions have led to a high level of maturity of digital public services, of which the majority are digital and accessible online.

The United States can learn a lot from Estonia on e-governance and, more specifically, on how to put in place the key enablers for a digitally enabled society: interoperability and digital identity. These enablers form an ecosystem in which to develop digital services and secure ways for citizens to access them online. Estonia successfully put in place these two enablers and, as a result, was able to spearhead the development of digital public services.

Digital identity, simply put, aims to establish a person’s unique identity, provide proof of that identity, and make it possible to assert that identity. [7]

Interoperability in this context refers to secure data interoperability between government and private sector databases and registries.

16.03.2021, Tallinn. The corona-positive Estonian Prime Minister Kaja Kallas made a presentation in the Riigikogu (Estonian parliament) via a video bridge. Credit: Photo Madis Veltman, Postimees

The last formal U.S. Digital Government Strategy, launched in 2012, sought to build "a 21st-century government that works better for the American people."[8] It conceptualized the layers (information, platform, and presentation) of digital services and overarching principles. A concept described under customer-centricity in the strategy is the key to achieving a whole-of-government approach in digital public services.

> Digital government should absorb the complexity of government on behalf of the citizen. The citizen does not have to know how the government is organized nor have to navigate a complex labyrinth of government structures to access and receive public services.

With a near totality of government services online, this is where Estonia excels.[9] These services are accessible location, device-independent, and in a way that most of the complexities of governance are hidden to the citizen.

Absorbing complexity means that public services are designed in a way that the citizen can conduct their activities without having to constantly switch between agencies for different forms or certificates. This should be solved in the backend systems and business processes of these organizations so that the citizen has a simpler experience through either a one-stop-shop model such as a citizen portal or through an agency portal that has made the necessary integrations with other stakeholders that are relevant in delivering the services they provide.

An Estonian citizen experiences government or e-governance primarily through the services they receive. The effectiveness and seamlessness of these services rely on having interoperability and digital identity as the building blocks in place. Absorbing the complexity of government means that the citizen does not have to spend time requesting, filing, and carrying papers from one agency to another in order to submit data that other parts of the administration already have and to prove their identity in ways that do not provide high levels of assurance or withstand the scrutiny of the information security community.

On top of the benefits for citizens, there are efficiency gains for the administration and private enterprise as a result of simplified reporting, receiving certificates, business licenses, and other documents necessary for operating and growing a business. Digital identity in Estonia saves about 2% of the GDP. [10] Interoperability saves about 1,400 years of working time annually.[11]

In the United States, the Office of Management and Budget (OMB), which serves the president in overseeing the implementation of their vision across the executive branch, is mindful of the federal government missing out on achieving digital transformation of the public sector. It cites poor management of technology investments and delayed implementation of projects that results in projects going live with outdated systems.[12]

The United States ranks relatively high in international e-government indices — e.g., it ranked ninth on the United Nations' E-Government Development Index. [13] While the availability of digital public services in the United States seems to be on the rise, there is still significant complexity the citizen has to bear to access public services digitally.

What Estonia Got Right

As mentioned above, Estonia was able to become a successful e-government due to the fact that it put in place key building blocks in a timely manner.[14] These building blocks helped Estonian citizens navigate the complexities of government.

The goal of e-governance is to provide digital services to citizens. Conceptually, the Estonian model considers the starting point for e-governance to be data, databases, and registries that contain specific information about individuals, businesses, and organizations. In some sense they form an economic cornerstone in the country because so many processes and services depend on their accuracy and availability.

The 2012 U.S. Digital Government Strategy was mindful about determining an information-centric approach. The Federal Data Strategy is looking to leverage federal data for the public good through principles, practices, and action steps. [15]The Federal Data Strategy, among several other ongoing initiatives, was laid out in the 2018 President's Management Agenda, which in effect sought to implement the GPRA Modernization Act of 2010.[16] [17]

The Federal Data Strategy is ambitious. It lays out 10 timeless principles, 40 practices for the next 5 to 10 years, and 20 action steps for the short term. In contrast, Estonia did not start with heavy strategies. The building blocks were designed in a way that they would be future-proof. The developments around services, portals, etc., were more project and purpose-based. This approach produced speed and agility.

While in Estonia the means to exchange data securely have been available since the early 2000s, a significant catalyst in actually spearheading the use of data across organizational boundaries was the introduction of the "once-only" principle — the government would only ask citizens once for the same information.[18] This means that if the government already knows a citizen's registered address, their education level, their tax identification number, that information should be sought from its custodian.

For this to work, agencies started acting as a single source of truth and as custodians of data (individual citizens being the proprietary owners of their data) in government based on their mission and mandate. Mission and mandate is especially relevant here, as many entities can benefit from the same data. That does not mean they should collect it themselves or duplicate it within their systems. The tax administration collects and maintains information related to taxation and vital events registries generate information regarding birth and death. As such, they should act as the source for that information.

A man casts his vote during general election at the polling station in Tallinn, Estonia March 3, 2019. REUTERS/Ints Kalnins

The concept of a single source of truth is achieved through policies and technology. Policies should look at the mandate of an organization: what the mission of that entity is and what related services the organization should provide or carry out to fulfill that mission. These services depend on either collecting and generating data or querying that data from other parts of the government. The choice between collecting or querying depends on how close that entity is to the source of the information (the individual or the business), their organizational capabilities, and the legal frameworks that surround them.

Security through Interoperability and Identity

Information is necessary to offer services to citizens in an effective and digital way, as the services often require combining data held at multiple organizational and legal boundaries. Legality and crossing organizational boundaries are significant components that feed into the need to design policy and systems in a security-by-design and a privacy-by-design fashion.

Historically, the exchange of information within government has been paper-based. Say, for example, official documents are carried via horse carriage from one city to another. The official receiving the documents needs to use them to make decisions based on their mission — things like granting a business license, denying social services, etc. These are activities that can create liability because there is room for error on behalf of the official. For the official to use the information they have received via horse carriage they need to trust its integrity. Usually, things like official letterheads, stamps, and signatures provided proof of integrity. The official would inspect them and the identity of the person delivering the documents, but they were most interested in executing against the mission of their organization and not making mistakes while doing so. If they did not trust the documents or the person delivering them, they would likely not use them.

Not a lot has changed in that regard. Agencies are still interested in executing the services and the business processes they have been mandated with and doing so in a way that does not create liability for them. They are not interested in making the postal network secure nor do they want to become experts in detecting document forgeries. This means that interoperability and secure data exchange are necessary at a nationwide level, but perhaps less so at an agency or mission level. [19]

Estonian policy and tech leaders understood this well. They created digital ecosystems that mimic how a democratic government already works, instead of redefining it through IT solutions. Understanding that data and its security is critical was one of the things Estonia got right: build the foundations in a secure-by-design way. [20]

A precinct worker checks a voter ID at the Bermuda precinct for the U.S. presidential election in Dillon, South Carolina, November 8, 2016. REUTERS/Randall Hill

While we seek to create a holistic experience for the citizen to receive public services, key enablers — government interoperability and secure data exchange, and digital identity, or secure authentication and digital signatures — must first be put in place. The first makes it possible to exchange data between independent organizations to create and offer complex services to citizens. The second makes it possible to access those services and provide consent in the form of digital signatures that carry legal meaning.

Implementing interoperability and secure data exchange requires not only the federal administration to work together, but also all the states to come on board because both levels of government need data from each other to design effective services. Not working in collaboration leads to a duplication of effort and data across all levels of government. This, eventually, results in a poor experience for the citizen and potentially nonconsensual collection of data.

Implementing digital identity starts with identity management and being able to uniquely identify an individual across systems, organizations, states, and jurisdictions. Countries that are able to manage the identities of their citizens can efficiently give out credentials or carriers of identity in physical or digital form and as a result build digital identity services on top of them. Today, in the United States the Social Security number is still widely used as a means of authentication for government services despite the leaks related to them.[21] [22] The most typical type of identity theft is applying for government benefits. [23]

For interoperability and digital identity to work, it is clear that data and records should be fully digitized. The United States aims to achieve this on a federal level by 2022 through M-19-21.[24] The challenge is that transitioning agencies have to maintain existing operations while building out new processes and that requires additional funding, which is often overlooked.[25]

Addressing Privacy Concerns

Another aspect that is relevant specifically from the citizen's perspective is privacy. [26] Countless organizations collect information about individuals who rarely have a say in what happens to that data: where and how it is processed and by whom. And on top of that, the data is usually duplicated across these organizations in a way that eventually the burden to prove accuracy of data falls on the individual.

Consent management mechanisms and platforms are relevant for citizens to give and revoke informed consent about who, how, and for what purpose and duration, uses their data.[27] Managing consent is not only relevant within the public sector, it becomes more so when private enterprise seeks to use data held at these organizations.

Registries and databases held by public sector entities formulate a vital economic building block. There are more ways in which the private sector can make use of these than we can imagine and it is possible to do so in a way that the citizen's privacy and the security of their data is not infringed upon.

For that to be fully feasible, citizens should also be able to track and monitor these activities. This will ensure greater transparency and accountability. If citizens give consent without being able to track what happens to their data they are unlikely to have full awareness and control over their privacy.

In Estonia, principles of data usage and consent were laid out in 1996 with the Personal Data Protection Act.[28] This was later supplemented by the General Data Protection Regulation (GDPR).[29] The GDPR enhanced data protection rules within the European Union (EU) to give people more control over their personal data and at the same time create a level playing field for businesses.

According to Article 6 of the GDPR, data processers can process personal data only if the person (a data subject) has given specific, unambiguous, and informed consent.[30] Requests for consent have to be in plain language, distinguishable from other matters, withdrawable by the data subject, and documented for evidence. EU citizens have mostly seen this through the flood of cookie consent requests when browsing websites. Despite the merits of the GDPR, it has arguably failed to stimulate economic activity because consent management and data usage monitoring tools have not been widely adopted. [31]

Illustration picture shows a fingerprint scanning device during the launch of the new eID, electronic identity card, Tuesday 14 January 2020, in Lokeren. BELGA PHOTO Nicolas Maeterlinck.

Like others around the world, U.S. citizens are concerned about their privacy. They sense that their control over and the transparency around how their data is used is decreasing.[32] The United States can learn a great deal in this regard from the GDPR, and more so from Estonia on how to put data protection and privacy to work so that the citizen does not only benefit on paper, but also in practice.

Does Estonia's Experience Apply to the United States?

While e-governance solutions cannot be directly transferred across countries, there are still a lot of things that can. Every country is unique in its culture, political dynamics, governance models (e.g., unitary or federal), people, political and business leaders, and the discourses they have. Yet principles of information security, good governance, and privacy by design are relatively universal across democratic countries. Approaches that have been designed based on universal principles are highly transferable and adaptable even to unique political and cultural settings.

Estonia is a small country. It has a unitary governance model, experienced occupation, and is a leader in e-governance and digitalization of society. The United States, on the other hand, is a large country. It has a federal system with a number of layers of governance and independence between those layers. It is largely private sector driven in terms of standards and is seen as the leader of the free world. Both Estonia and the United States are democratic countries with distribution of power, transparent policymaking, and due process, to name a few characteristics.

Distribution of power is especially relevant when developing a digital government as there is not only distribution between the three branches, but also within the executive. There are political and policy mandates, organizational boundaries that different parts of the federal government, states, departments, and municipalities have. This is something that the Estonian approach to e-governance has understood and taken inspiration from — to avoid centralization between the branches but more so even within the executive.

X-Road, which has since 2001 been the solution that drives e-Estonia, is based on the principles of decentralization and distribution.[33] The assumption is that every organization has a mandate that sets out its mission and, as a result, the services it provides and the data it collects (for which it acts as a single source of truth) or needs (which it seeks from other organizations that act as a single source of truth) for those services.

White House Office of Management and Budget (OMB) acting director Shalanda Young testifies on President Biden's 2022 budget during a hearing of the House Budget Committee on Capitol Hill in Washington, U.S. June 9, 2021. REUTERS/Jonathan Ernst

The interoperability platform acts as an ecosystem of trusted counterparts. After the coordinating body has accepted an organization, the organization implements a standardized security gateway for data exchange. Exchanging data in this distributed model is done peer-to-peer, organization-to-organization. Data does not flow through any intermediaries or centralized message hubs. Organizations establish service-level agreements between each other to agree what kind of data, for what purpose and scope, is to be exchanged and what the obligations are of both sides. [34]

The exchange of a particular piece of data is based on access control lists. As a result, an organization can only query a defined "data service" that provides it with the information it needs to execute a business process.

All of these transactions are logged, digitally signed, and time stamped to provide long-term proof of value, auditability, and non-repudiation among other principles.

Building an e-state, e-government founded on democratic principles, and building an e-kingdom, e-government founded on non-democratic principles, require different approaches. [35] While they are different in many ways, the United States and Estonia are like-minded democratic countries.

A Question of Scalability

A key concern that policymakers might have is one of scalability: can something that works in a country of 1.3 million work in a country of 330 million?

First off, population size does not pose scalability issues for the approach on interoperability, as it's been designed to scale to any size of ecosystem and does not rely on centralized components. The digital identity approach scales with hardware. It's important to keep in mind that the building blocks that Estonia put in place are meant to work in a whole-of-government approach. Cities, states, federal government have business processes that in large part rely on each other and without bridging that the U.S. will struggle to achieve the necessary network effects of e-governance.

The answer lies in design choices taken around how these solutions are architected and implemented. One of the key principles of these solutions has always been scalability so that the overall ecosystem can grow and meet the needs of tens, hundreds, or thousands of organizations when it comes to interoperability and a million, tens of millions, or hundreds of millions of people when it comes to digital identity. The motive of scalability is necessary to uphold both from a scalability of governance perspective as well as a scalability of infrastructure perspective.

It is also worth noting that the principles implemented in Estonia are no longer purely Estonian. Many countries, some with relatively large populations, have either taken inspiration or directly copied the models used in Estonia to their countries.

One of the largest and most successful transfers of Estonia's interoperability model in Europe (in addition to Finland and Iceland) can be found in Ukraine (population 45 million) in its Trembita.[36] In Africa, this model has been implemented in several countries, including Tunisia and Benin[37] (both countries have a population of around 12 million). In the Americas, it is being piloted on a national level in Colombia (population 50 million) and on state levels in Mexico (population 128 million). In Asia, it is being implemented in Malaysia (population 32 million) and several other countries.

Lessons for Policymakers from Estonia's Experience

The challenges around e-governance are not unique to the United States. Rather, they are universal in public administration and governance. The solutions to these challenges exist and have been executed well in many countries.

Specific e-governance solutions are a reflection of the policy principles that they are designed to carry out. When designed well and based on democratic principles, these solutions can be adopted and effectively scaled to a country that is the size of the United States or one the size of Estonia.

To promote a more effective and efficient e-governance in the United States, this policy brief makes three recommendations on (1) lead agency, (2) interoperability and the use of data, and (3) identity, secure authentication, and digital signatures.

On Lead Agency

While there are several stakeholders, starting from political and business leaders driving the debate to policymakers condensing that into policy, these solutions are typically not properly implemented. The Estonian example has shown while part of everyone's mission should be to make government work better, there has to be an entity responsible for it. In the U.S. context that could mean empowering the General Services Administration (GSA with political will and leadership and providing it adequate funding to build the necessary foundation for e-governance.[38]

On Interoperability and Use of Data

Federal, state, and local governments must adopt a once-only policy. The Office of Management and Budget (OMB) should initiate this process with federal CIOs as a catalyst and expand to state and local government stakeholders. The National Association of State Chief Information Officers could be used as a channel to coordinate policy adoption between states. In addition, the Federal Data Strategy should aim to reduce duplication of data within the federal government by clearly indicating how specific parts of the administration are mandated by policy and mission to collect, maintain and share data.

Under the once-only policy, public entities have to enforce internal procedures and systems to act as sole verification sources for the data they collect and maintain. OMB must enforce strict guidelines for federal departments and agencies while state CIOs engage local governments.

Sharing data should be allowed only based on legal compliance and rights and only for the purpose of the service the data is needed for. That means you can only "ask for" / query a slice of the data based on access rights.

The 21st Century Integrated Digital Experience Act should be expanded to clearly state that data has to flow between the counterparts that are part of service flows and business processes and avoid central intermediaries through which data is transferred. All of these queries should be logged for auditing and non-repudiation so that they can be used in disputes and to prevent/respond to misuse of data (e.g., querying someone's data without a legal basis).

All levels of governance have to provide adequate control mechanisms so that citizens can monitor how their data is being used by public and private sector organizations. In addition to monitoring data access, data custodians have to develop procedures under which citizens can grant, revoke and monitor consent to private sector organizations to access their data held by public organizations.

At a bare minimum, the General Services Administration needs to provide a framework under which public sector entities can implement the solutions for interoperability and secure data exchange. Entities should adopt secure components for interoperability and data exchange that are standardized and interoperable – GSA together with OMB

A man poses for photographer as he enters a PIN code for a new German ID card (Personalausweis) inserted into a card reader, in Berlin, October 27, 2010. The card can be ordered from November 1 and offers a new so-called eID (electronic Identity). REUTERS/Fabrizio Bensch

must define a set of open standards for interoperability and secure data exchange so that every entity doesn't have to develop their own. While doing so, they must keep in mind how the private sector could provide these tools to public sector entities based on the agreed standards and rules.

Dedicated funding has to be allocated by Congress and state legislatures for developing these standards, implementing pilot projects together with the private sector and to support the transition period where organizations move from existing services and business processes to new ones.

On Identity, Secure Authentication, and Digital Signatures

Every individual should have a simple way to prove their identity and have a unique identifier tied with them that grants them uniqueness. This identifier should not be a secret (such as the SSN) and ideally not include sensitive information (e.g., sex, age, etc.). U.S. National Center for Health Statistics, U.S. Census Bureau, NASCIO, and state CIOs have to agree on a uniform birth certificate format that includes the assignment of unique identifiers to citizens. This process has to be adamantly supported by the federal government and through political leadership.

The U.S. must adopt a stock-and-flow model for assigning unique identifiers, so that while citizens are gradually given identifiers, newborns are assigned with a unique identifier at birth. A stock-and-flow model means that two parallel processes have to be put in place: 1) onboarding the existing population (stock) by assigning them unique identifiers and 2) enabling hospitals and Vital Events Registrars to assign unique identifiers to newborns (flow) that are tied to birth certificates and the identifiers of the newborn's parents. The identifier is tied to the individual from birth and stays with the individual after death and is used on identification documents such as ID cards, passports, driver's licenses. State CIOs and legislatures have to increase the capacity of vital records registrars with this new mandate and ensure that all vital statistics registries are digitized and powered by modern ICT capabilities.

These unique identifiers should be used universally in all government systems so that data about a person in registries and databases is tied to the unique identifier – a person's information would be queried using their unique identifier instead of their first name and last name; or as a combination of both. OMB and the federal government must support and incentivize the states to modernize their vital records management capacity and systems. Federal departments and agencies should pilot the transition to using unique identifiers with a few states and later expand on that success.

The Biden Administration must support the adoption of unique identifiers as a core pillar of identity management. OMB must also develop a roadmap on how these unique identifiers are incorporated into the systems and business processes of the federal government.

Bibliography

"21st Century Integrated Digital Experience Act." 2019. Digital.gov. November 1, 2019. https://digital.gov/resources/21st-century-integrated-digital-experience-act/.

Aslanova, T. 2021 "The Role and Importance of Consent Management in Public Organizations in the Digital Age: Case on Estonia"

Ansper, Arne. 2001. "E-State from a Data Security Perspective." https://cyber.ee/research/theses/arne_ansper_msc.pdf.

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information." Pew Research Center: Internet, Science & Tech. November 15, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Briefing Centre. 2012a. "E-Estonia." E-Estonia. 2012. https://e-estonia.com/.

2012b. "ID-Card." E-Estonia. 2012. https://e-estonia.com/solutions/e-identity/id-card.

Daniel Wu and Sam Catania. 2021. "Hackers Leak Social Security Numbers, Student Data in Massive Data Breach." The Stanford Daily. April 1, 2021

European Commission. 2018a. "Personal Data Protection Act – Riigi Teataja." Www.riigiteataja.ee. December 12, 2018. https://www.riigiteataja.ee/en/eli/523012019001/consolide.

2018b. "X-Road – Cross-Border Co-Development of National Data Exchange Platform-Projects." Ec.europa.eu. January 26, 2018. https://ec.europa.eu/regional_policy/en/projects/europe/x-road-cross-border-co-development-of-national-data-exchange-platform.

2019. "Data Protection." Europa. 2019. https://ec.europa.eu/info/law/law-topic/data-protection_en.

European Parliament. 2018. "Article 6 EU General Data Protection Regulation (EU-GDPR)." Www.privacy-Regulation.eu. September 5, 2018. https://www.privacy-regulation.eu/en/article-6-lawfulness-of-processing-GDPR.htm.

Federal Data Strategy." n.d. Strategy.data.gov. https://strategy.data.gov/overview/.

Heller, Nathan. 2017. “Estonia, the Digital Republic.” The New Yorker. December 11, 2017. https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

Insurance Information Institute. 2014. “Facts + Statistics: Identity Theft and Cybercrime.” Iii.org. 2014. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

Jackson, Eric. 2020. “The Right Mix: Estonia Ensures Privacy and Access to E-Services.” Estonian World. June 2, 2020. https://estonianworld.com/security/right-mix-estonia-ensures-privacy-access-e-services-digital-age/.

Kelam, Mari-Ann. 2021. “The Role of the United States in the Restoration of Estonia’s Independence.” Estonian World. July 4, 2021. https://estonianworld.com/life/role-united-states-restoration-estonias-independence/.

Lani, Marit. n.d. “Data Exchange Platform for Benin.” The Government of Benin. Accessed July 15, 2021. https://ega.ee/project/data-exchange-platform-benin/.

Lechner, Paul. 2020. “GDPR: Three Ways the World Has Changed in the Privacy Law’s First Two Years.” CPO Magazine. July 7, 2020. https://www.cpomagazine.com/data-protection/gdpr-three-ways-the-world-has-changed-in-the-privacy-laws-first-two-years/.

Nast, Condé. n.d. “Welcome to E-Stonia, the World’s Most Digitally Advanced Society.” Wired UK. Accessed July 15, 2021. https://www.wired.co.uk/article/digital-estonia.

Office of E-Government & Information Technology. n.d. “Office of E-Government & Information Technology.” The White House. Accessed July 15, 2021. https://www.whitehouse.gov/omb/management/egov/#A3.

Office of Management and Budget, The Executive Office of the President. n.d. “Digital Government: Building a 21st Century Platform to Better Serve the American People.” Archives.gov. https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html.

2019. “Memorandum for Heads of Executive Departments and Agencies.” White House. June 28, 2019. https://www.whitehouse.gov/wp-content/uploads/2019/08/M-19-21-new-2.pdf.

Pop, Valentina. 2015. “[Interview] ‘You Can’t Use 18th Century Law for a Digital World.’” EUobserver. February 26, 2015. https://euobserver.com/economic/127800.

Schneider, Troy K. 2021. “The Long Road to Electronic Records Management -.” FCW. February 16, 2021. https://fcw.com/articles/2021/02/16/fcw-perspectives-erm-long-road.aspx.

Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber. 2017. “Equifax Says Cyberattack May Have Affected 143 Million in the U.S.” The New York Times. September 7, 2017

“Головна.” n.d. Trembita.gov.ua. Accessed July 15, 2021. https://trembita.gov.ua/ua.

Trump Administration. 2018. “Presidents Management Agenda.” Www.performance.gov. 2018. https://trumpadministration.archives.performance.gov/PMA/PMA.html.

United Nations. 2020. “UN E-Government Development Index.” Un.org. 2020. https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/184-United-States-of-America.

U.S. Congress. 2010. “GPRA MODERNIZATION ACT of 2010.” https://www.congress.gov/111/plaws/publ352/PLAW-111publ352.pdf.

Vassil, Kristjan. 2016. “Digital Dividends Estonian E-Government Ecosystem: Foundation, Applications, Outcomes.” http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf.

Veldre, Anto. 2016. “Introduction of X-Tee | Estonian Information System Authority.” Republic of Estonia. February 2016. https://www.ria.ee/en/state-information-system/x-tee/introduction-x-tee.html.

Whyte, Andrew, ed. 2019. “Iceland Latest Nation to Adopt Estonia’s X-Road Platform.” ERR. February 28, 2019. https://news.err.ee/915067/iceland-latest-nation-to-adopt-estonia-s-x-road-platform.

X-TEE. 2021. “X-TEE FACTSHEET EE.” www.x-Tee.ee. July 2021. https://www.x-tee.ee/factsheets/EE/#eng.

Endnotes

1 Office of Management and Budget, The Executive Office of the President. n.d. "Digital Government: Building a 21st Century Platform to Better Serve the American People." Archives.gov. https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html.

2 Mazmanian, Adam. 2021. "Lawmakers press for IDEA Act adoption" FCW May 6, 2021 https://fcw.com/articles/2021/05/06/idea-act-letter-oversight.aspx

3 "21st Century Integrated Digital Experience Act." 2019. Digital.gov. November 1, 2019. https://digital.gov/resources/21st-century-integrated-digital-experience-act/.

4 Nast, Condé. n.d. "Welcome to E-Stonia, the World's Most Digitally Advanced Society." Wired UK. Accessed July 15, 2021. https://www.wired.co.uk/article/digital-estonia.

5 Kelam, Mari-Ann. 2021. "The Role of the United States in the Restoration of Estonia's Independence." Estonian World. July 4, 2021. https://estonianworld.com/life/role-united-states-restoration-estonias-independence/.

6 Heller, Nathan. 2017. "Estonia, the Digital Republic." The New Yorker. December 11, 2017. https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic.

7 World Bank ID for Development, ID 101: Basic Concepts https://id4d.worldbank.org/guide/id-101-basic-concepts-0 Accessed July 31 2021

8 Office of Management and Budget, The Executive Office of the President. n.d. "Digital Government: Building a 21st Century Platform to Better Serve the American People." Archives.gov. https://obamawhitehouse.archives.gov/sites/default/files/omb/egov/digital-government/digital-government.html.

9 Briefing Centre. 2012a. "E-Estonia." E-Estonia. 2012. https://e-estonia.com/.

10 Briefing Centre. 2012b. "ID-Card." E-Estonia. 2012. https://e-estonia.com/solutions/e-identity/id-card.

11 X-TEE. 2021. "X-TEE FACTSHEET EE." Www.x-Tee.ee. July 2021. https://www.x-tee.ee/factsheets/EE/#eng.

12 Office of E-Government & Information Technology. n.d. "Office of E-Government & Information Technology." The White House. Accessed July 15, 2021. https://www.whitehouse.gov/omb/management/egov/#A3.

13 United Nations. 2020. "UN E-Government Development Index." Un.org. 2020. https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/184-United-States-of-America.

14 Vassil, Kristjan. 2016. "Digital Dividends Estonian E-Government Ecosystem: Foundation, Applications, Outcomes." http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf.

15 "Federal Data Strategy." n.d. Strategy.data.gov. https://strategy.data.gov/overview/.

16 Trump Administration. 2018. "Presidents Management Agenda." Www.performance.gov. 2018. https://trumpadministration.archives.performance.gov/PMA/PMA.html.

17 U.S. Congress. 2010. "GPRA MODERNIZATION ACT of 2010." https://www.congress.gov/111/plaws/publ352/PLAW-111publ352.pdf.

18 Pop, Valentina. 2015. "[Interview] 'You Can't Use 18th Century Law for a Digital World.'" EUobserver. February 26, 2015. https://euobserver.com/economic/127800.

19 An organization with a singular view on their mission can in principle build the necessary ad-hoc integrations and authentication tools, collect duplicates of data and develop digital services through that. From a whole-of-government perspective, that is a waste of resources.

20 Ansper, Arne. 2001. "E-State from a Data Security Perspective." https://cyber.ee/research/theses/arne_ansper_msc.pdf.

21 The Stanford Daily. 2021. "Hackers Leak Social Security Numbers, Student Data in Massive Data Breach." https://www.stanforddaily.com/2021/04/01/hackers-leak-social-security-numbers-student-data-in-massive-data-breach/

22 The New York Times. 2017. "Equifax Says Cyberattack May Have Affected 143 Million in the U.S." https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?_r=0/

23 Insurance Information Institute. 2014. "Facts + Statistics: Identity Theft and Cybercrime." Iii.org. 2014. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

24 Office of Management and Budget, The Executive Office of the President. 2019. "Memorandum for Heads of Executive Departments and Agencies." White House. June 28, 2019. https://www.whitehouse.gov/wp-content/uploads/2019/08/M-19-21-new-2.pdf.

25 Schneider, Troy K. 2021. "The Long Road to Electronic Records Management -." FCW. February 16, 2021. https://fcw.com/articles/2021/02/16/fcw-perspectives-erm-long-road.aspx.

26 Jackson, Eric. 2020. "The Right Mix: Estonia Ensures Privacy and Access to E-Services." Estonian World. June 2, 2020. https://estonianworld.com/security/right-mix-estonia-ensures-privacy-access-e-services-digital-age/.

27 Aslanova, T. 2021. "The Role and Importance of Consent Management in Public Organizations in the Digital Age: Case on Estonia"

28 European Commission. 2018. "Personal Data Protection Act – Riigi Teataja." Www.riigiteataja.ee. December 12, 2018. https://www.riigiteataja.ee/en/eli/523012019001/consolide.

29 European Commission. 2019. "Data Protection." Europa. 2019. https://ec.europa.eu/info/law/law-topic/data-protection_en.

30 European Parliament. 2018a. "Article 6 EU General Data Protection Regulation (EU-GDPR)." Www.privacy-Regulation.eu. September 5, 2018. https://www.privacy-regulation.eu/en/article-6-lawfulness-of-processing-GDPR.htm.

31 Lechner, Paul. 2020. "GDPR: Three Ways the World Has Changed in the Privacy Law's First Two Years." CPO Magazine. July 7, 2020. https://www.cpomagazine.com/data-protection/gdpr-three-ways-the-world-has-changed-in-the-privacy-laws-first-two-years/.

32 Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information." Pew Research Center: Internet, Science & Tech. November 15, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

33 Veldre, Anto. 2016. "Introduction of X-Tee | Estonian Information System Authority." Republic of Estonia. February 2016. https://www.ria.ee/en/state-information-system/x-tee/introduction-x-tee.html.

34 The data provider usually agrees to data quality and availability requirements, while the data user agrees to some limitations of data processing, privacy and security

35 Ansper, Arne. 2001. "E-State from a Data Security Perspective." https://cyber.ee/research/theses/arne_ansper_msc.pdf.

36 European Commission. 2018b. “X-Road – Cross-Border Co-Development of National Data Exchange Platform-Projects.” Ec.europa.eu. January 26, 2018. https://ec.europa.eu/regional_policy/en/projects/europe/x-road-cross-border-co-development-of-national-data-exchange-platform. Whyte, Andrew, ed. 2019. “Iceland Latest Nation to Adopt Estonia’s X-Road Platform.” ERR. February 28, 2019. https://news.err.ee/915067/iceland-latest-nation-to-adopt-estonia-s-x-road-platform. “Головна.”.” n.d. Trembita.gov.ua. Accessed July 15, 2021. https://trembita.gov.ua/ua.

37 Lani, Marit. n.d. “Data Exchange Platform for Benin.” The Government of Benin. Accessed July 15, 2021. https://ega.ee/project/data-exchange-platform-benin/.

38 Riotta, Chris. June 10 2021. “Biden’s Pick to Lead GSA: ‘We Can’t Implement Government Policy If We Can’t Get The Damn Websites To Work”.

Center for European Policy Analysis
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004
info@cepa.org | www.cepa.org